This record is a partial extract of the original cable. The full text of the original cable is not available.

C O N F I D E N T I A L SECTION 01 OF 07 DJIBOUTI 001007

SIPDIS

Dept for IRM/OPS/ITI/SI/CSB; DJIBOUTI For RIMC

E.O. 12958: DECL: 1.6 (X1)
TAGS: ACKM ACOA KRIM
SUBJECT: COMMUNICATIONS SECURITY AUDIT - Djibouti (A-116)

Classified by William B. Mills, IRM/OPS/ITI/SI/CSB Communication Security Auditor, reason 1.5(C)

¶1. (U) This telegram contains the results of the COMSEC audit conducted by State Auditor William B. Mills with the COMSEC custodian Charles E. Fleenor in Djibouti on October 7, 2005. The auditor will forward the results of this audit to the COMSEC account manager Kelly Walters at the Central Office of Record (COR).

¶2. (C) Please reconcile the Inventory Report associated with this Audit report and notify post by telegram.

¶3. (U) Post has been advised to retain a copy of this audit until completion of the next audit.

¶4. (U) There are only two ratings assigned to COMSEC Audits: satisfactory or unsatisfactory. A satisfactory rating has been assigned to this audit.

¶5. (U) The following items (numbers correspond to the audit questions) are:

¶A. Deficiencies found and corrected during the audit: 4, 12, 18B, 53
¶B. Deficiencies found and require post's corrective action: 1, 3, 8, 36A, 52, 59
¶C. Other recommendations: 25, 29, 31, 64 A/B

AUDITOR COMMENTS:

Post STE's are using 2.0 software. Post should coordinate installation of 2.4 software with RIMC Pretoria.

¶6. (C) The Custodian must address the deficiencies noted in paragraph 5.B."within 30 days" from the date of this telegram and report telegraphically the corrective actions taken.

¶1. Did the auditor account for each item on the Special Inventory?

( ) YES (x) NO ( ) N/A

COMMENT: USFAU 33310 880103 4103 4783420 not accounted for. COR representative is aware of situation and is contacting previous custodian for a destruction report.

RECOMMENDATION: Post should continue cooperation with COR representative and previous custodian to resolve issue.

¶2. What is the transaction number assigned to the audit inventory?
TN-30

¶3. Check the Short Title, Edition, and Registry of the keying material in use, does it match the effective status of the S/KAF?

( ) YES (X) NO ( ) N/A

COMMENT: USKAU H3794 ED: 3 Destroyed under TN-15. Post is now using Ed: 4.

RECOMMENDATION: Post should cable SI/CSB with this change.

¶A. Is all COMSEC keying material located at post, listed on the S/KAF?

(x) YES ( ) NO ( ) N/A

¶4. Is superseded keying material being destroyed within 72 hours of supersession?
(5 FAH-6 H-411 i.)

( ) YES (x) NO ( ) N/A

COMMENT: Corrected on spot.

¶5. With the exception of Secure Voice Equipment, are there any Type I encryption devices, installed outside the controlled access areas (CAA)?
(12 FAM 974.8-2, 94 state 175008)

( ) YES (x) NO ( ) N/A

¶A. Are the encryption devices being keyed higher than unclassified?

SIPDIS

( ) YES ( ) NO (x) N/A

¶6. Are accountable COMSEC publications (publications listed on the SF-153 inventory) page checked upon receipt (i.e., Transfer and Hand-Receipt), after posting of amendments, and upon changes of custodians? (5 FAH-6 H-316.4)

( ) YES ( ) NO (x) N/A

¶A. Does the account hold COMSEC accountable publications but not the associated COMSEC equipment? If YES, list the publications and advise the COMSEC custodian to request disposition from the Department's vault.

( ) YES (x) NO ( ) N/A

¶7. Select an accountable COMSEC publication and perform a page check. Identify short title and serial number of the publication.

Note: The following manuals are COMSEC accountable and should be held by post, if the respective equipment is installed.

KAO 168 - Operations manual for KY-58
KAM 366 - Maintenance Manuel for KY-57

¶A. Is the publication complete? (5 FAH-6 H-132)

( ) YES ( ) NO (x) N/A

COMMENT: Post should hold KAM-366 - Maintenance Manual for KY-57. This manual was requested and is enroute to post per 05 State 185091.

¶B. Have all amendments been entered?

( ) YES ( ) NO (x) N/A

¶8. Does the account hold unaccountable manuals for COMSEC equipment?

Note: The following manuals are not COMSEC accountable and should be held by post if the respective equipment is installed:

LMM-2a - Maintenance/operations manual for KG-84c
LMM-5a - Maintenance/operations manual for KG-84/84a
KAO 218 - Operations manual for KG-194

( ) YES (x) NO ( ) N/A

RECOMMENDATION: As post has KG-84A's in its inventory it should request a copy of the LMM-5A from its COR representative.

¶9. Does the post hold the most recent (2000) Communication Security Handbook 5 FAH-6?

(x) YES ( ) NO ( ) N/A

¶10. If Data-Cryptors installed at post, are they operated in the secure mode? (5 FAH-6 H-224.d)

(x) YES ( ) NO ( ) N/A

¶11. Are all off-site State circuits, such as warehouses, Financial Management Centers, commercial buildings, Consular offices, etc., encrypted with approved DES encryption? (5 FAH-6 H-230)

(x) YES ( ) NO ( ) N/A

COMMENT: Post has wireless circuit to embassy warehouse that uses SafeNet encryption.

¶12. Is there a memorandum from the RSO/PSO listing the authorized classification level of all Secure Voice Equipment at the post? (5 FAH-6 H-561 c.)

( ) YES (x) NO ( ) N/A

COMMENT: Corrected on spot.

RECOMMENDATION:

¶13. Have all mandatory modifications, as listed below, been installed on COMSEC equipment? (5 FAH-6 H-136)

(x) YES ( ) NO ( ) N/A

The following devices require modification (s):
KG-84/84A mods 1, 2, 3
KY-57/58 Mod 2

¶14. Is Secure Voice Equipment sealed properly? If not, list Short Title and Registry number.

(x) YES ( ) NO ( ) N/A

¶15. Is unused Secure Voice Equipment keying material (seed keys and KOV 14 cards) still in its protective packaging? (99 STATE 191301)

(x) YES ( ) NO ( ) N/A

¶16. Are excess zeroized STU-III keys returned to the department's vault? (5 FAH-6 H-562)

(x) YES ( ) NO ( ) N/A

¶17. Select several STU-III crypto ignition keys (CIK's) and STE KOV 14 cards, insert into STU-III or the associated STE, and display the contents. Do not select unused keys sealed in protective packages:

¶A. Does the display indicate the CIK is a fill device? If YES, what is the short title and Registry No. of the key, and is it on the audit inventory?

( ) YES (x) NO ( ) N/A

¶B. Does the display indicate the CIK or KOV 14 is personalized, (i.e. Agency, and geographic location of the COMSEC account)? (5 FAH-6 H-227.2.6)

(x) YES ( ) NO ( ) N/A

¶C. Does the account hold unused non-personalized Secure Voice Equipment key material? (91 State 336382)

( ) YES (x) NO ( ) N/A

¶18. Is there any COMSEC material on hand receipt? (5 FAH-6 H-323)

(x) YES ( ) NO ( ) N/A

¶A. Select several hand receipts: are hand receipts completed IAW the example in 5 FAH-6 H-323 Exhibit H-323.1? (5 FAH-6 H-323.1 a.)

(x) YES ( ) NO ( ) N/A

¶B. Is the "I, certify" statement on all hand receipts?

( ) YES (x) NO ( ) N/A

COMMENT: Statement was omitted from a few hand receipts.

RECOMMENDATION: Corrected on spot.

Note: Statement should read as follows: " I, the undersigned, certify that I am aware of the special safeguard for cryptographic equipment and material and will apply those safeguards to the above listed item(s)."

¶C. Is the equipment physically sight checked and re-certified with the semi-annual inventory?
(5 FAH-6 H-323.1 f.)

(x) YES ( ) NO ( ) N/A

¶D. Does present hand receipt holder have the keying material and an approved security safe to store the material? (5 FAH-6 H-323.1 d.)

(x) YES ( ) NO ( ) N/A

¶19. If COMSEC material has been transferred to or from a COMSEC account other than the Department Vault, did the Central Office of Record authorize the transfer? (5 FAH-6 H-133)

( ) YES ( ) NO (x) N/A

¶20. Is there a memorandum or telegram on file from the local security office certifying that the PCC meets physical security standards? (for info purposes only)
(5 FAH-6 H-316.1 (4))

(x) YES ( ) NO ( ) N/A

COMMENT: Dated Oct. 1, 2005

¶21. Is there a current authorized entry list for the PCC
(5 FAH-6 H-124.4-1 a.)

(x) YES ( ) NO ( ) N/A

¶22. Is there a visitor's register and is it being utilized? (5 FAH-6 H-124.4 -1 a., 12 FAM 663.3-1 d.)
(x) YES ( ) NO ( ) N/A

¶23. Is cryptographic equipment covered or hidden when uncleared personnel are present? (5 FAH-6 H124.4-7 b. (1))

(x) YES ( ) NO ( ) N/A

¶24. Is personally owned audio, electronic, and video equipment prohibited from being stored or used in the COMSEC facility? (5 FAH-6 H-521 e. (4))

(x) YES ( ) NO ( ) N/A

¶25. Is there a current JF-47 on file, i.e., COMSEC Officer, Custodian, alternate(s), and Appointing Officer are still assigned to the post? (5 FAH-6 H-313.1)

( ) YES (x) NO ( ) N/A
COMMENT: A corrected JF-47 to TN-21 is in signature process.

¶A. Is the JF-47 completed IAW the example in the 5 FAH-6? (5 FAH-6 H-313 Exhibit H-313.1)

(x) YES ( ) NO ( ) N/A

¶B. Do the COMSEC Custodian and all alternates have cryptographic access? (5 FAH-6 H-123.2 c.)

(x) YES ( ) NO ( ) N/A

¶26. Does post have a copy of the latest Department cable (05 State 6887) and subsequent amendments that provide cryptographic security clearances of personnel?

(x) YES ( ) NO ( ) N/A

¶27. Is the TN log current and complete? (5 FAH-6 H-326 a.)

(x) YES ( ) NO ( ) N/A

¶28. Is there a copy of all SF-153 transactions for the past year and current year?

(x) YES ( ) NO ( ) N/A

¶29. Is there a copy of the most recent SF-153 inventory report on file? (5 FAH-6 H-325.1 a. & b.)

( ) YES (x) NO ( ) N/A

COMMENT: Semi-annual inventory held to be done in conjunction with audit inventory with COR knowledge. There was one item on the inventory in contention and COR resolution received with audit.

¶30. Is the Central Office of Record reconciliation message attached to the latest inventory? (5 FAH-6 H-325.2 b.)

( ) YES ( ) NO (x) N/A

¶31. Are semi-annual inventories being completed and returned to the Central Office of Record within 10 working days? (5 FAH-6 H-325.2 a.)

( ) YES (x) NO ( ) N/A

RECOMMENDATION: Needs to be done.

¶32. Is post performing a Change of Custodian Inventory upon the appointment of a new Custodian? (5 FAH-6 H-325.3)

(x) YES ( ) NO ( ) N/A

Comment: Last change of custodian inventory was 05 State 140509, of August 7, 2005. This inventory has not bee reconciled due to submission of improper JF-47. A new JF-47 is in process and will be submitted ASAP.

¶33. Is COMSEC keying material stored in a GSA approved class 5 or 6 safe?(5 FAH-6 H-521 g.)

(x) YES ( ) NO ( ) N/A

COMMENT: Current cryptographic keying material is kept in:
Mosler Safe, Model no. 406225 00A 09, Serial no. 1210510 - Class 6

All other cryptographic keying is kept in:
Mosler Safe, Model no. 41625500A09 , Serial no. 1520085 Class 6

¶34. Is post conducting the daily COMSEC Inventory to sight check

material stored in the COMSEC safe(s) each time the safe(s) is(are) opened? (Form DS 1962 or similar forms may be used for document of the Daily inventory) (5 FAH-6 H-316.2)

(x) YES ( ) NO ( ) N/A

¶35. Are the combinations for the COMSEC safes and PCC stored in a class 5 or 6 safe? (12 FAM 532.2-2)

(X) YES ( ) NO ( ) N/A

COMMENT: Same as second safe question 33.

¶36. Are combination security container cards, form SF-700 (replaced OF-111), posted inside the COMSEC safe?
(12 FAM 532.2-2)

(x) YES ( ) NO ( ) N/A

¶A. Has the COMSEC safe combination been changed within the past 12 month and/or upon change of assigned personnel? (12 FAM, Appendix E, 972)

( ) YES (x) NO ( ) N/A

COMMENT: Combinations last changed 05-01-2004

RECOMMENDATION: Combination change for ComSec safe and vault door should be scheduled asap.

¶B. Are all personnel that have access to safe listed on SF-700 and are they still at this post? (12 FAM 532.2-4 c.)

( ) YES (x) NO ( ) N/A

COMMENT: Will be corrected with 36A.

¶37. Are Security Container Check Sheets, SF-702 posted on the outside of the COMSEC safe and are being utilized to document the opening/closing of the safe?
(12 FAM 539.1 c.)

(x) YES ( ) NO ( ) N/A

¶38. Are Activity Security Checklists, SF-701 posted and utilized in the PCC to insure that all COMSEC assets are properly stored and safeguarded, locking devices are secured, and alarm systems are activated?
(5 FAH-6 H-522, 12 FAM 664.8-4 a., 12 FAM 534.2-1)

(x) YES ( ) NO ( ) N/A

¶39. Is all COMSEC material inspected for tampering or compromise before opening?(5 FAH-6 H-134 & H-324, 99 STATE 191301)

(x) YES ( ) NO ( ) N/A

¶40. Is all COMSEC material received inventoried immediately after opening? (5 FAH-6 H-324)

(x) YES ( ) NO ( ) N/A

¶41. ARE SEGMENT DISPOSITION/USAGE RECORDS (DS 3089) FOR CANISTER KEY MATERIAL UTILIZED? (5 FAH-6 H-411 H.)

(x) YES ( ) NO ( ) N/A

¶A. DO TWO PERSONS INITIAL THE DESTRUCTION COLUMN?
(5 FAH-6 H-411 h.)

(x) YES ( ) NO ( ) N/A

¶B. Are segments of key material destroyed immediately after use?
(5 FAH-6 H-124.3-3 (2), 5 FAH-6 H-411 g.)

(x) YES ( ) NO ( ) N/A

¶42. Are Destruction Reports prepared on SF-153 signed by two persons?(5 FAH-6 H-411 h.)

(x) YES ( ) NO ( ) N/A

¶43. Are monthly destruction reports being submitted to the Central Office of Record within 5 working days of destruction? (5 FAH-6 H-412 b.)

(x) YES ( ) NO ( ) N/A

¶44. Check several past STU-III key destruction reports.

¶A. Are destruction reports for STU-III keys that have been loaded/zeroized submitted within 30 days? (5 FAH-6 H-412.b.)

(x) YES ( ) NO ( ) N/A

¶B. Are destruction reports for STU-III seed keys prepared IAW published instructions (i.e. the remark column indicating either a zeroized STU-III key or the STU-III terminal serial number)?(5 FAH-6 H-227.3)

(x) YES ( ) NO ( ) N/A

¶45. Is COMSEC material destroyed using approved destruction device (s)? What is the make/Model of the destruction device (s)? (5 FAH-6 H-422.1)

(x) YES ( ) NO ( ) N/A

Make Model
SEM 1012 Disintegrator (serial no. 11308)
SEM 266 Shredder

¶46. If post has a disintegrator(s), are both 3/8" and 3/32" disintegrator screens at post? (5 FAH-6 H-422.2 (b))

(x) YES ( ) NO ( ) N/A

¶47. Is logo tape being disposed of properly? (5 FAH-6 H-134 exhibit H-134 d, c and d.)

(x) YES ( ) NO ( ) N/A

¶48. Does post have an Emergency Destruction Plan (EDP)? Provide the date of the EDP. (5 FAH-6 H-431 a.)

(x) YES ( ) NO ( ) N/A

EDP Date: 01/16/2005

¶49. Is the EDP incorporated into the post's Emergency Action Plan?(12 FAM 664.7-2 a.)

(x) YES ( ) NO ( ) N/A

¶50. Does the EDP identify by the chain of command the officers authorized to order implementation of the EDP?
(5 FAH-6 H-433)

(x) YES ( ) NO ( ) N/A

¶51. Are assigned tasks listed by duty station rather than by the name of a person? (5 FAH-6 H-432 b.)

(x) YES ( ) NO ( ) N/A

¶52. Does the EDP describe the destruction of each type of COMSEC material and equipment at post? (5 FAH-6 H-432 e.)

( ) YES (x) NO ( ) N/A

RECOMMENDATION: Post needs to include STE and KG-235 destruction info in EDP.

¶53. EDP emergency destruction drills conducted (every three months or upon change in Information Resource Management personnel) under supervision of the Administrative OR Security officer and documented? (IMO may be utilized only in the event of unavailability of the primary officers)(5 FAH-6 H-432 c.)

( ) YES (X) NO ( ) N/A

COMMENT: Corrected on spot.

¶54. Does the EDP list the special tools required to destroy the material and equipment? (5 FAH-6 H-432 exhibit H-434.2)

(x) YES ( ) NO ( ) N/A

¶55. Does post have the special tools for emergency destruction of COMSEC material? (5 FAH-6 H-434 Exhibit 434.2)

(x) YES ( ) NO ( ) N/A

¶A. Are tools readily available and in the vicinity of the equipment for emergency destruction? (5 FAH-6 H-434.2)

(x) YES ( ) NO ( ) N/A

¶B. Are the tools kept in a sealed separate tool kit or wall mounted unit designated for emergency destruction only? (5 FAH-6 H-434.2 a.)
(x) YES ( ) NO ( ) N/A

¶C. Are the emergency destruction tools in good condition? (5 FAH-6 H-434.2 b.)

(x) YES ( ) NO ( ) N/A

¶56. Does the EDP list by short title and the priority in which material and equipment are to be destroyed? (5 FAH-6 H-432 f.)

(x) YES ( ) NO ( ) N/A

¶57. Does the EDP incorporate what to destroy under possible or precautionary emergency conditions?
(5 FAH-6 H-434.4)
(x) YES ( ) NO ( ) N/A

¶58. Does the EDP incorporate what to do under final emergency destruction? (5 FAH-6 H-435)

(x) YES ( ) NO ( ) N/A

¶59. Does the EDP contain instructions for evacuating all nonessential COMSEC equipment/material to a safe haven at the first sign of overrun threat precautionary emergency conditions? (5 FAH-6 H-434.4)

( ) YES (x) NO ( ) N/A

COMMENT: EDP addresses communications and systems software only.

RECOMMENDATION: EDP safehaven info needs to be expanded to include ComSec equipment/material.

¶60. Does the EDP cover the reporting of material destroyed during an emergency? (5 FAH-6 H-436)

(x) YES ( ) NO ( ) N/A

¶61. Does the EDP identify components and/or circuit boards by equipment (KG-84, KG-194, and STU/STE, NES devices, etc.) That must be destroyed prior to evacuating post?
(5 FAH-6 H-435)

(x) YES ( ) NO ( ) N/A

¶62. Does the EDP provide for entry of foreign nationals, uncleared American personnel, fire fighters,/medical attendants to restricted area (s) during emergencies?
(5 FAH-6 H-124.4-2)

(x) YES ( ) NO ( ) N/A

¶63. Is there a copy of the last COMSEC audit at post and have all deficiencies from past audit been satisfactorily resolved?(5 FAH-6 H-612.3)

(X) YES ( ) NO ( ) N/A

¶64. Correspondence:

¶A. Is there any outstanding, unanswered correspondence from the Central Office of Record to post? If YES, list correspondence and comment on delay.

(x) YES ( ) NO ( ) N/A

COMMENT: A corrected JF-47 (TN-21) is in the signature process and will be submitted to COR upon receipt from Ambassador's office.

¶B. Are there any outstanding issues, correspondence, concerns or recommendations that the COMSEC Custodian would like to make about the Department's COMSEC program?

(x) YES ( ) NO ( ) N/A

COMMENT: (A) Post understands that COR representative is in touch with last ComSec Custodian from post to determine whether missing crypto key USFAU 33310 880103 4103 4783420 was actually destroyed, and if so will request a signed destruction report. If last custodian cannot verify destruction of key, COR is planning to issue FS-507 - ComSec Security Violation. Please keep post appraised of any progress ref this item.